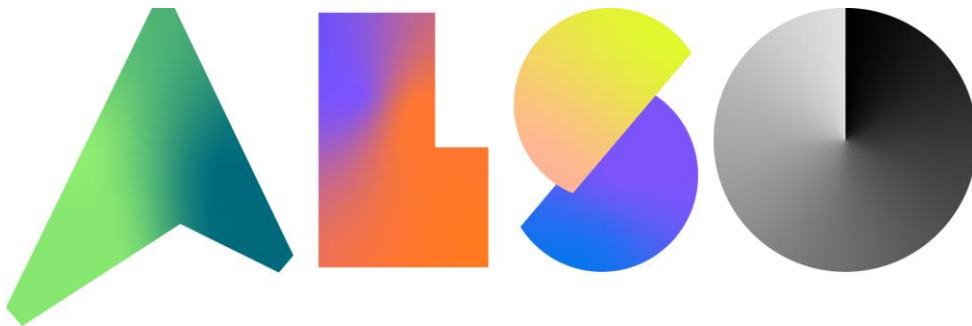


**How to Fortinet .....**

**Konfiguration eines IPsec VPN-Tunnel zwischen einer FortiGate und Checkpoint SNB Firewall**



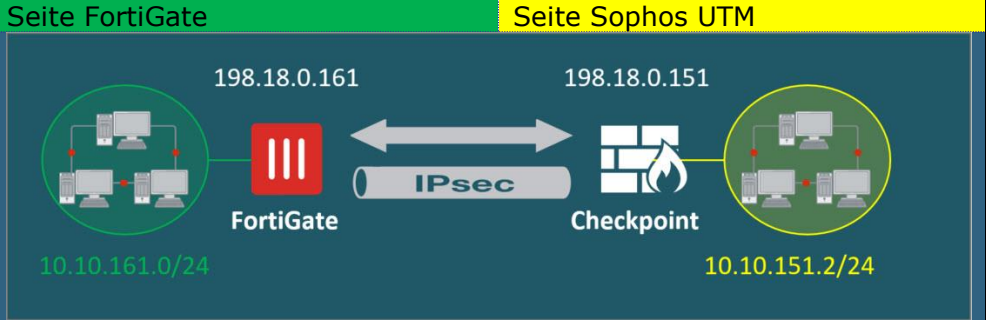


## Inhaltsverzeichnis

<b>KONFIGURATION EINES IPSEC VPN-TUNNEL ZWISCHEN EINER FORTIGATE UND CHECKPOINT SNB FIREWALL.....</b>	<b>1</b>
INHALTSVERZEICHNIS .....	2
AUSGANGSLAGE .....	3
KONFIGURATION AUF DER FORTIGATE 60F .....	4
Konfigurieren des VPN Tunnels über das Webgui: .....	4
Netzwerkeinstellungen:.....	4
Authentication konfigurieren: .....	5
Phase 1 Parameter konfigurieren: .....	5
Phase 2 Selektoren konfigurieren: .....	6
Konfigurieren der Routen: .....	7
Konfigurieren der Policies:.....	7
Konfigurieren des VPN Tunnels über die CLI: .....	9
VPN Phase 1 konfigurieren: .....	9
endVPN Phase 2 konfigurieren: .....	9
Routen konfigurieren:.....	9
Adress Objekte für Policies konfigurieren: .....	9
Policy konfigurieren:.....	10
KONFIGURATION AUF DER CHECKPOINT 1550 .....	11
Einen neuen Tunnel erstellen:.....	11
Netzwerk Parameter:.....	12
Authentication konfigurieren: .....	12
Remote Site Encryption Domain konfigurieren .....	13
Encryption für Phase 1 und Phase 2 konfigurieren: .....	14
Advanced Optionen konfigurieren:.....	15
Konfigurieren eines Netzwerk Objektes: .....	15
Konfigurieren der Policy: .....	16
Regelset Anordnung: .....	17
ERFOLGSKONTROLLE : .....	18
VPN Monitor auf der FortiGate : .....	18
VPN Monitor auf dem Checkpoint Gerät: .....	18
Traffic von vom Fortinet Netz zum Checkpoint Netz : .....	18
FortiGate diag debug flow funktion:.....	19
Checkpoint fw monitor funktion: .....	20

## Ausgangslage

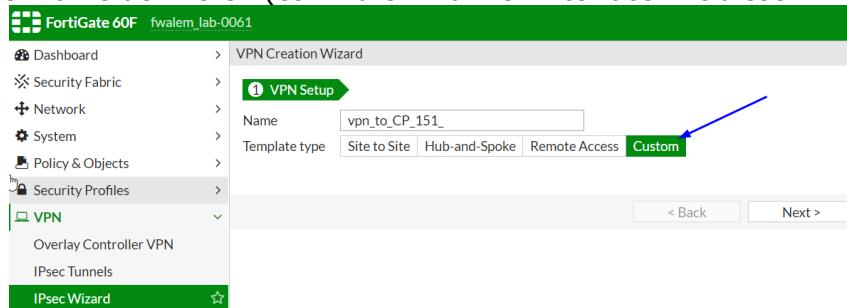
In diesem Dokument wird beschrieben, wie ein Site-to-Site VPN zwischen einer FortiGate und einer Checkpoint SNB Firewall konfiguriert werden kann. Dieses Setup wurde unter folgenden Bedingungen aufgebaut und durchgetestet:

	Seite FortiGate	Seite Sophos UTM
<b>Netzplan</b>		
<b>Hardware</b>	FortiGate 60F	Checkpoint 1550
<b>Software</b>	4.6.2 build1723	R80.20.05 (992001134)
<b>Lokales Netzwerk</b>	10.10.161.0/24	10.10.151.0/24
<b>Public IP-Adresse</b>	198.18.0.161	198.18.0.151
<b>Authentication</b>	Pre-shared Key definieren	
<b>IKE Version</b>	Version 2	
<b>Phase 1 Proposal</b>	Algorithms: AES256-SHA256 DH-Group 15	
<b>Phase 1 Key Lifetime</b>	86400 Sekunden	
<b>Phase 2 Proposal</b>	Algorithms: AES256-SHA256 DH-Group 15	
<b>Phase 2 Key Lifetime</b>	3600 Sekunden	

## Konfiguration auf der FortiGate 60F

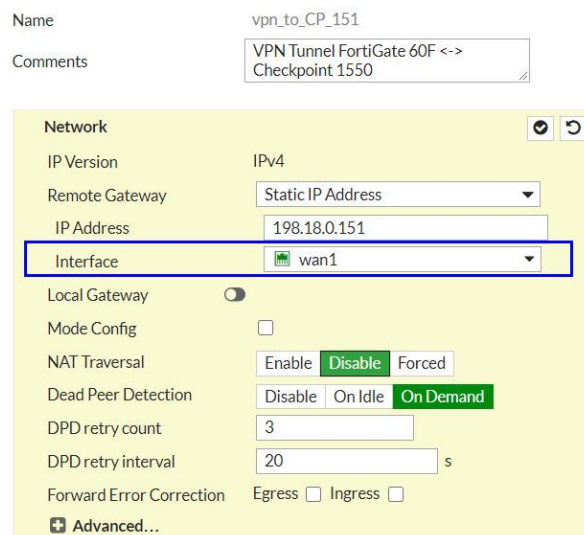
### Konfigurieren des VPN-Tunnels via WebGUI:

1. Über das Menü *VPN* → *IPsec Tunnels* → *IPsec Tunnel* wird ein neuer Tunnel erstellt
2. Auf den Reiter *Custom* klicken um den Wizard zu umgehen
3. VPN-Tunnel Name definieren (es wird ein Tunnel-Interface mit diesem Namen generiert)



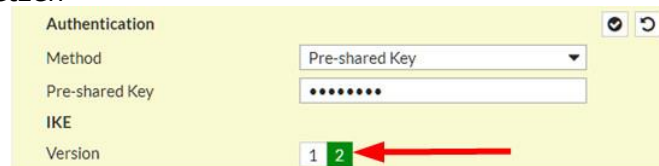
### Netzwerkeinstellungen:

1. Bei *Remote Gateway* den Typ auf *static IP Address* setzen
2. Im Feld *IP Address* wird die öffentliche IP-Adresse der Checkpoint eingetragen (198.18.0.151)
3. Bei *Interface* wird das ausgehende Interface (meistens WAN) angegeben. Auf diesem Interface wird das Tunnel-Interface dann automatisch als Sub-Interface angelegt.
4. *NAT Traversal* ist noch zu definieren, falls ein NAT Device zwischen der FortiGate und der Checkpoint vorhanden ist.



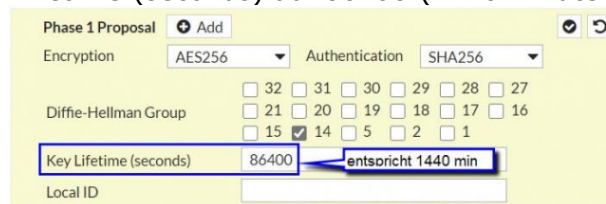
### Authentication konfigurieren:

1. *Method* auf *Pre-shared Key* einstellen
2. Im Feld *Pre-shared Key* einen komplexen, nicht nachvollziehbaren Key konfigurieren (dieser Key wird auf der Checkpoint dann auch benötigt)
3. In unserem Beispiel werden wir mit IKE Version 2 arbeiten. Dementsprechend den Parameter auf 2 setzen



### Phase 1 Parameter konfigurieren:

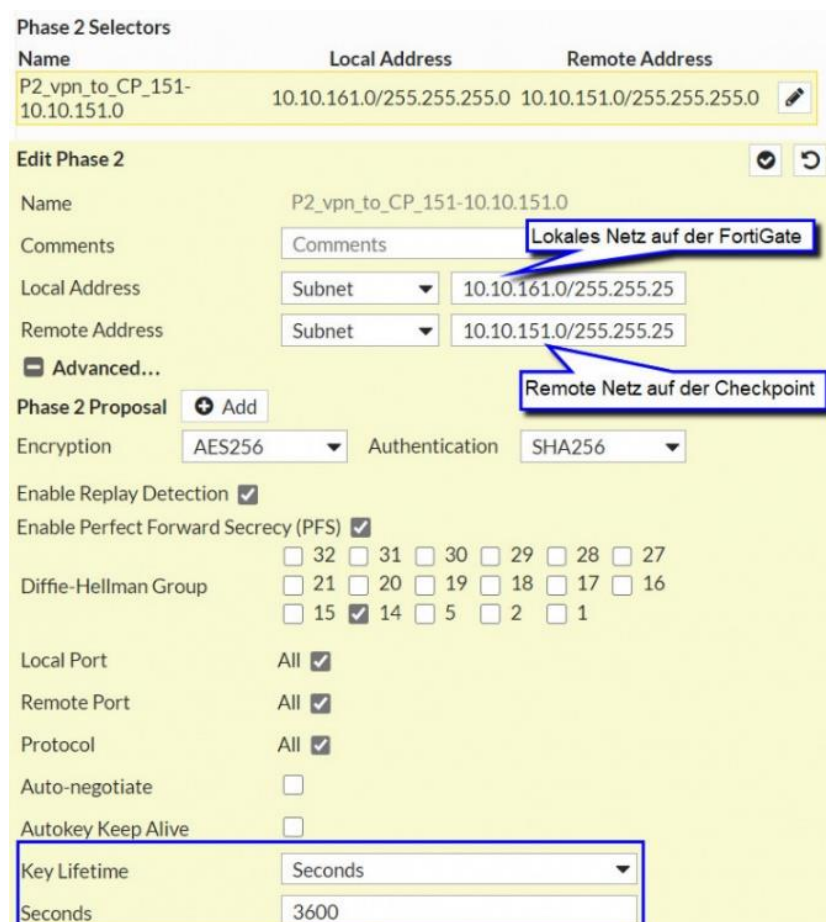
1. *Encryption* auf *AES256* und *Authentication* auf *SHA256* konfigurieren
2. Alle anderen Encryption- und Authentication-Parameter entfernen (X anwählen)
3. Die *Diffie-Hellman Group* wird auf *14* eingestellt
4. Der Parameter *Key Lifetime (seconds)* auf *86400* (1440 Minuten) stellen



## Phase 2 Selektoren konfigurieren:

In diesem Beispiel zeigen wir, wie man den Selektor für 10.10.161.0/24 zu 10.10.151.0/24 konfiguriert:

1. *Name* in diesem Feld kann ein Name für den Selektor definiert werden
2. *Local Address* Das Netz welches bei der Fortigate erreicht werden soll. Typ auf *Subnet* stellen und die Adresse: 10.10.161.0/24 konfigurieren
3. *Remote Address* Das Netz, welches wir hinter der Checkpoint erreichen wollen. Typ auf *Subnet* stellen und Adresse 10.10.151.0/24 konfigurieren
4. Unter dem Menüpunkt *Advanced* können die Phase 2 Proposal konfiguriert werden
5. *Encryption* auf *AES256* und *Authentication* auf *SHA256* stellen. Alle anderen Encryption- und Authentications-Parameter entfernen
6. *Perfect Forward Secrecy (PFS)* aktivieren
7. Die *Diffie-Hellman Group* auf *14* einstellen
8. *Key Lifetime* auf *Second* stellen und dann den Wert *3600* Sekunden setzen (dies ist nicht der Default-Wert der FortiGate).



**Phase 2 Selectors**

Name	Local Address	Remote Address
P2_vpn_to_CP_151-10.10.151.0	10.10.161.0/255.255.255.0	10.10.151.0/255.255.255.0

**Edit Phase 2**

Name: P2\_vpn\_to\_CP\_151-10.10.151.0

Comments: Comments

Local Address: Subnet 10.10.161.0/255.255.25

Remote Address: Subnet 10.10.151.0/255.255.25

**Advanced...**

Phase 2 Proposal: Add

Encryption: AES256 Authentication: SHA256

Enable Replay Detection: ☒

Enable Perfect Forward Secrecy (PFS): ☒

Diffie-Hellman Group: ☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27 ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☒ 14 ☐ 5 ☐ 2 ☐ 1

Local Port: All ☒

Remote Port: All ☒

Protocol: All ☒

Auto-negotiate: ☐

Autokey Keep Alive: ☐

Key Lifetime: Seconds

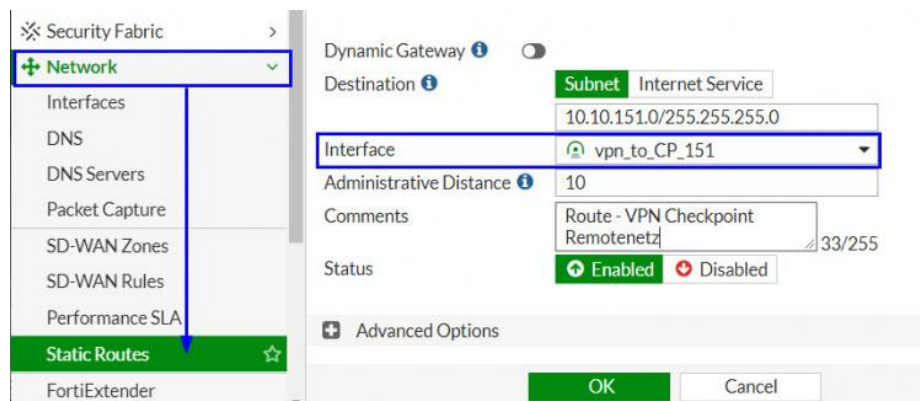
Seconds: 3600

### Konfigurieren der Routen:

Auf der FortiGate muss das Netz der Remote-Seite (10.10.151.0/24) in den IPSec-Tunnel geroutet werden. Dabei zeigt die Route auf das Tunnel-Interface (vpn\_to\_CP\_151). Damit bei einem Unterbruch des Tunnels der Traffic nicht über die Default-Route ins Internet geroutet wird, sollte eine Blackhole Route konfiguriert werden.

Die Routen werden folgendermassen konfiguriert: Menu: *Network* → *Static Routes* → 

### Route Remote Netz:

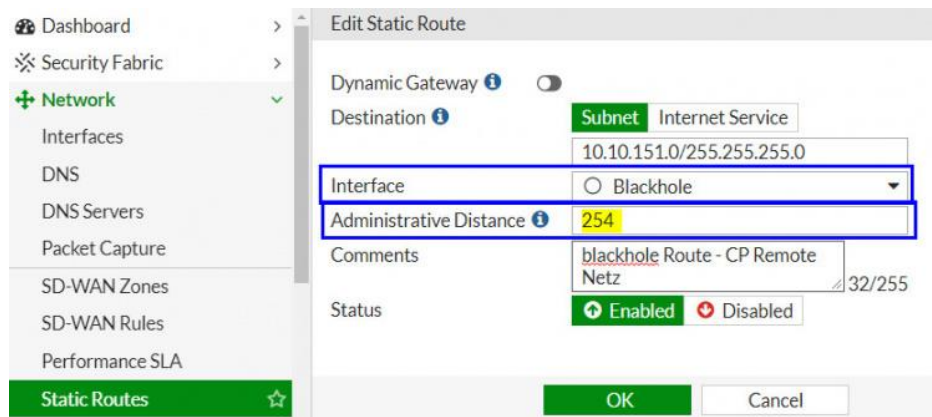


The screenshot shows the 'Static Routes' configuration page in the FortiGate web interface. The left sidebar has 'Network' expanded, and 'Static Routes' is selected. The main configuration area shows:

- Dynamic Gateway:** Disabled
- Destination:** Subnet, 10.10.151.0/255.255.255.0
- Interface:** vpn\_to\_CP\_151
- Administrative Distance:** 10
- Comments:** Route - VPN Checkpoint Remotenetz
- Status:** Enabled

At the bottom, there are 'OK' and 'Cancel' buttons.

### Blackhole Route:




The screenshot shows the 'Edit Static Route' page in the FortiGate web interface. The left sidebar has 'Network' expanded, and 'Static Routes' is selected. The main configuration area shows:

- Dynamic Gateway:** Disabled
- Destination:** Subnet, 10.10.151.0/255.255.255.0
- Interface:** Blackhole
- Administrative Distance:** 254
- Comments:** blackhole Route - CP Remote Netz
- Status:** Enabled

At the bottom, there are 'OK' and 'Cancel' buttons.

### Konfigurieren der Policies:


Es braucht mindestens eine Policy auf der FortiGate. Damit der Traffic bidirektional durch den Tunnel geht, empfiehlt es sich eine Regel in jede Richtung zu konfigurieren. Dabei ist die Kommunikation zwischen dem VPN-Tunnel Interface (vpn\_cp-forti) und dem internen Interface (internal2).


Menu : *Policy & Objects* → *IPv4 Policy* → 



**Policy 1 : Zugriff 10.10.151.0/24 → 10.10.161.0/24**

ID 5



Name ⓘ l\_vpn\_CP\_151->10.0.161.0-24

Incoming Interface  vpn\_to\_CP\_151


Outgoing Interface  userlan-client (internal2)



Source  net\_remoteVPN-10.10.151.0-24   
+



Negate Source ☐

Destination  net\_ul-10.10.161.0-24   
+

Negate Destination ☐

Schedule  always

Service  ALL   
+

Action  ACCEPT  DENY

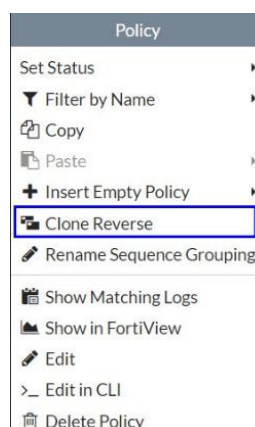
Inspection Mode **Flow-based** Proxy-based

Firewall / Network Options

NAT ☐









**Policy 2 : Zugriff 198.18.0.0/24 → 192.168.111.0/24**

Die ganze Policy noch bei Bedarf gegengleich konfigurieren (Source Interface / Netz und Destinations Interface / Netz) gegengleich konfigurieren. Dabei kann die *Clone Reverse* Funktion benutzt werden.



Die Regel muss einfach noch eingeschaltet werden, sonst ist sie inaktiv.

**Regelset :**

Policy										
Name	From	To	Source	Destination	Service	Action	NAT	Security Profiles	Log	Bytes
l_vpn_CP_151->10.0.161.0-24	 vpn_to_CP_151	 userlan-client (internal2)	 net_remoteVPN-10.10.151.0-24	 net_ul-10.10.161.0-24	ALL	ACCEPT	Disabled	no-Inspection	All	0B
o_vpn_10.10.161.0-24->CP_151	 userlan-client (internal2)	 vpn_to_CP_151	 net_ul-10.10.161.0-24	 net_remoteVPN-10.10.151.0-24	ALL	ACCEPT	Disabled	no-Inspection	All	0B



## Konfigurieren des VPN-Tunnels über die CLI:

### VPN Phase 1 konfigurieren:

```
config vpn ipsec phase1-interface
edit "vpn_to_CP_151"
    set interface "wan1"
    set ike-version 2
    set peertype any
    set net-device disable
    set proposal aes256-sha256
    set dhgrp 14
    set remote-gw 198.18.0.151
    set psksecret "Hier_einen_komplexen_Key_eingeben"
next
end
```

### VPN Phase 2 konfigurieren:

```
config vpn ipsec phase2-interface
    edit "p2-vpn_to_lab-0062-10.10.162.0-24"
        set phase1name "vpn_to_lab-0062"
        set proposal aes256-sha256
        set dhgrp 14
        set auto-negotiate enable
        set src-subnet 10.10.161.0 255.255.255.0
        set dst-subnet 10.10.162.0 255.255.255.0
    next
end
```

### Routen konfigurieren:

```
config router static
    edit 2
        set dst 10.10.151.0 255.255.255.0
        set device "vpn_to_CP_151"
    next
    edit 3
        set dst 10.10.151.0 255.255.255.0
        set distance 254
        set comment "blackhole Route - CP Remote Netz"
        set blackhole enable
    next
end
```

### Adress-Objekte für Policies konfigurieren:

```
config firewall address
    edit "net_remoteVPN-10.10.151.0-24"
        set comment "Remote Netz -VPN Checkpoint"
        set color 10
        set subnet 10.10.151.0 255.255.255.0
    next
    edit "net_ul-10.10.161.0-24"
        set color 3
        set subnet 10.10.161.0 255.255.255.0
    next
end
```

**Policy konfigurieren:**

```
config firewall policy
  edit 5
    set name "I_vpn_CP_151->10.0.161.0-24"
    set srcintf "vpn_to_CP_151"
    set dstintf "internal2"
    set srcaddr "net_remoteVPN-10.10.151.0-24"
    set dstaddr "net_ul-10.10.161.0-24"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
  next
  edit 6
    set name "O_vpn_10.10.161.0-24->CP_151"
    set srcintf "internal2"
    set dstintf "vpn_to_CP_151"
    set srcaddr "net_ul-10.10.161.0-24"
    set dstaddr "net_remoteVPN-10.10.151.0-24"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
  next
end
```

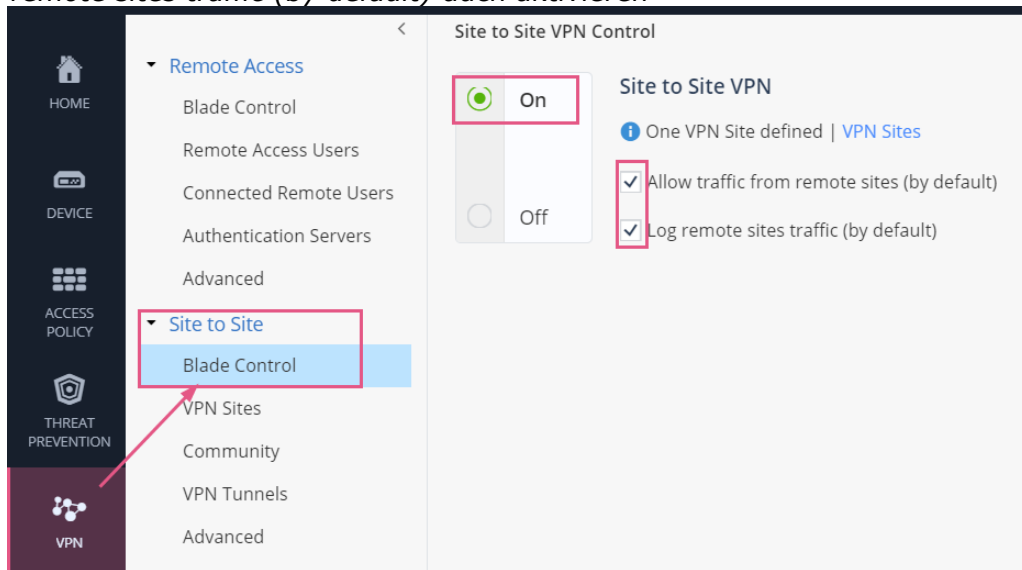
## Konfiguration auf der Checkpoint 1550

Auf der Checkpoint SNB Firewall wird ein VPN wie folgt konfiguriert:

Zuerst müssen wir gewährleisten, dass die Checkpoint den VPN Traffic akzeptiert:

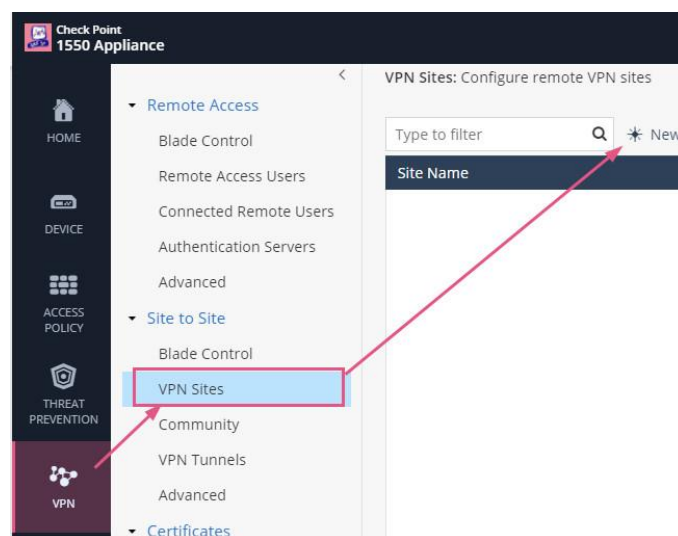
Dies wird unter im Menü unter *VPN* → *Site-to-Site* → *Blade Control* konfiguriert:

1. Den Regler auf *On* stellen
2. *Allow traffic from remote sites (by default)* muss angewählt sein
3. Wenn man im Log die Verbindungen sehen will, (was sehr zu empfehlen ist) die Option *Log remote sites traffic (by default)* auch aktivieren



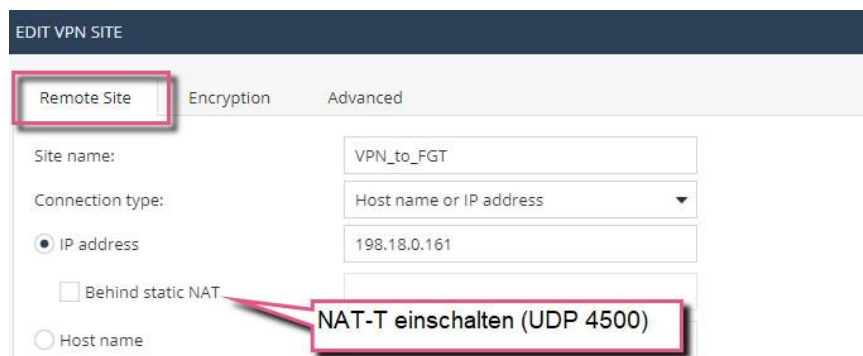
### Einen neuen Tunnel erstellen:

Unter dem Menü *VPN* → *VPN Sites* →  kann ein neuer Tunnel erfasst werden.



**Netzwerk Parameter:**


1. Auf das TAB *Remote Site* gehen
2. *Site name*: Hier wird der Name des VPN Tunnels definiert
3. Bei *Connection type* auf *Host Name or IP address* setzen
4. *IP address* anwählen und im Feld die öffentliche IP-Adresse der FortiGate eingeben (198.18.0.153)
5. *Behind static NAT* ist die NAT Traversal-Einstellung

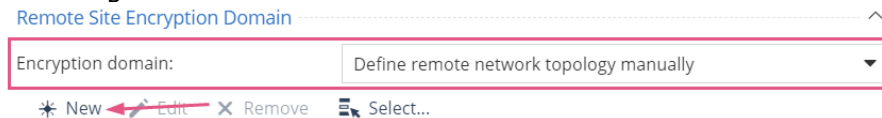
**Authentication konfigurieren:**

1. *Pre-shared secret* anwählen (entspricht der Option Pre-shared KEY auf der FortiGate)
2. Im Feld *Password* den Key eingeben, welcher bereits auf der FortiGate gewählt wurde
3. *confirm* noch einmal den Key eingeben







## Remote Site Encryption Domain konfigurieren:


1. Die *Remote Site Encryption Domain* entspricht dem lokalen Netz auf der FortiGate bei den Selektoren
2. Zuerst muss das Netz oder der Host definiert werden. Dafür auf den  **New** klicken
3. Es öffnet sich folgendes Fenster:

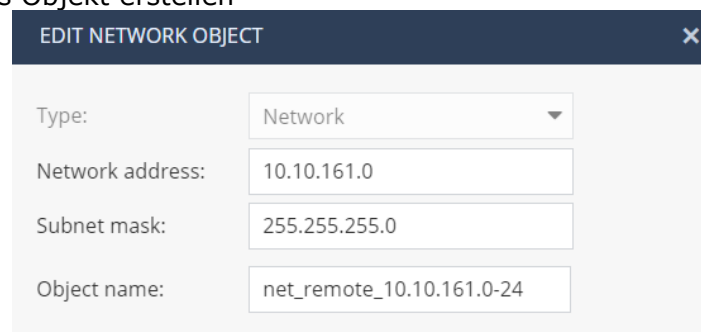


Remote Site Encryption Domain

Encryption domain: Define remote network topology manually

 New  Edit  Remove  Select...

1. Den *Type* auf *Network* stellen
2. *Network address*: Die Netzadresse angeben (ohne Subnetzmaske) in unserem Fall das Netzwerk auf der FortiGate 10.10.161.0
3. *Subnetmask*: Die Subnetzmaske des Netzes angeben: 255.255.255.0
4. *Object name* Hier wird der Name definiert, wie das Objekt danach ausgewählt werden kann
5. Mit  **Apply** das Objekt erstellen




EDIT NETWORK OBJECT

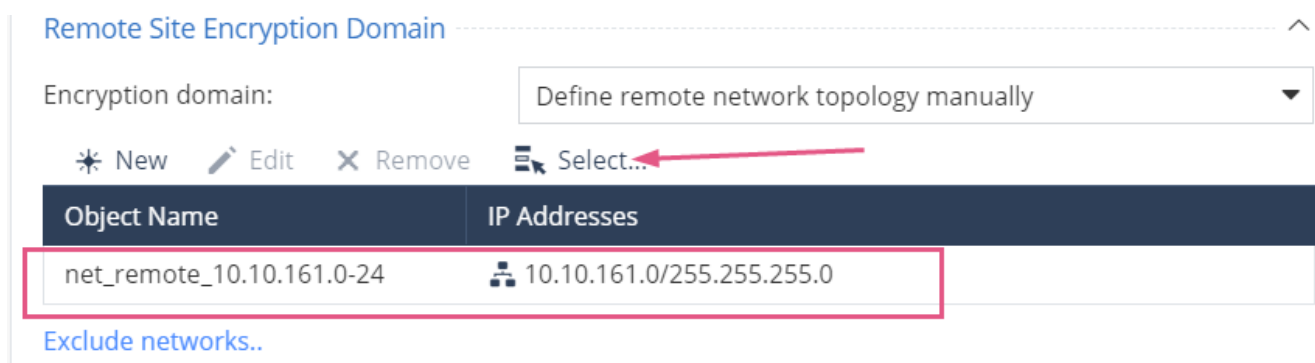
Type: Network

Network address: 10.10.161.0

Subnet mask: 255.255.255.0





Object name: net\_remote\_10.10.161.0-24


Mit  **Select...** kann das Adressobjekt zu der Encryption Domain hinzugefügt werden:



Remote Site Encryption Domain

Encryption domain: Define remote network topology manually

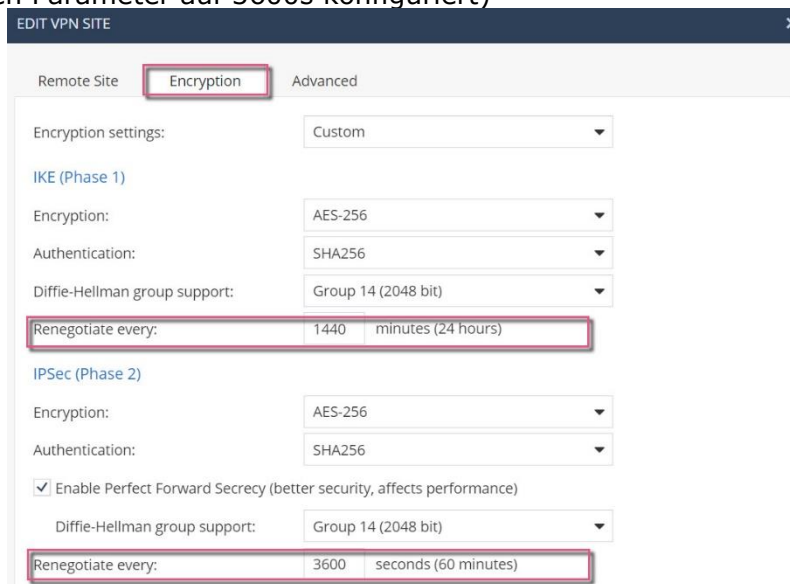
 New  Edit  Remove  Select...

Object Name	IP Addresses
net_remote_10.10.161.0-24	 10.10.161.0/255.255.255.0

[Exclude networks..](#)

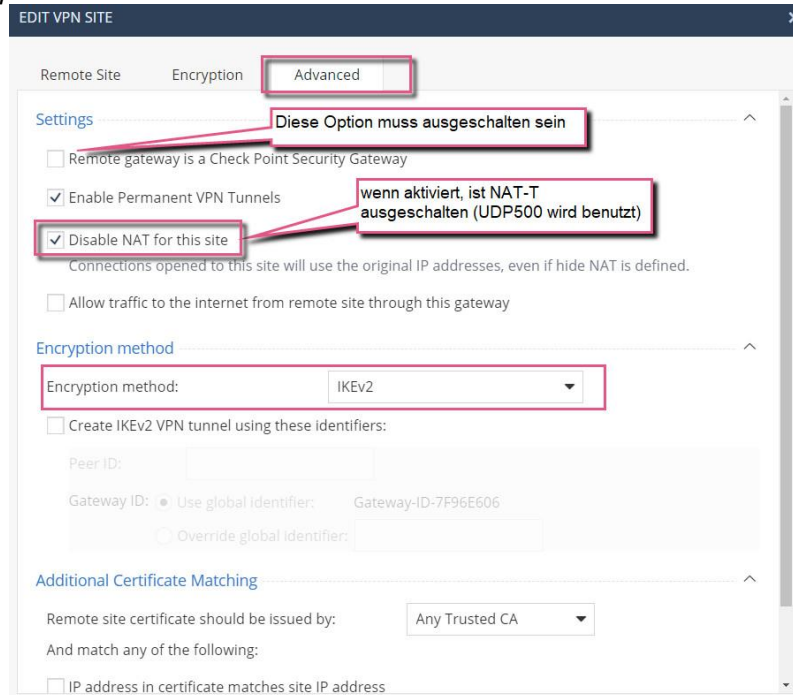
**Encryption für Phase 1 und Phase 2 konfigurieren:**

1. Das TAB *Encryption* anwählen
2. *Encryption settings* auf *custom* stellen
3. IKE (Phase 1)
  - a. *Encryption* auf *AES-256* konfigurieren, alle anderen Parameter deaktivieren
  - b. *Authentication* auf *SHA256* konfigurieren, alle anderen Parameter ebenfalls deaktivieren
  - c. *Diffie-Hellman group support* setzen wird auf *Group 14 (2048 bit)*
  - d. *Renegotiate every*: wird auf 1440 Minuten gesetzt (auf der FortiGate ist 86400 Sekunden eingestellt, was 1440 Minuten entspricht)
4. IPSec (Phase2)
  - a. *Encryption* auf *AES-256* konfigurieren, alle anderen Parameter deaktivieren
  - b. *Authentication* auf *SHA256* konfigurieren, alle anderen Parameter ebenfalls deaktivieren
  - c. *Enable Perfect Forward Secrecy (PFS)* aktivieren
  - d. *Diffie-Hellman group support* setzen wir auf *Group 14 (2048 bit)*
  - e. *Renegotiate every*: wird auf 3600 Sekunden gesetzt (auf der FortiGate haben wir diesen Parameter auf 3600s konfiguriert)



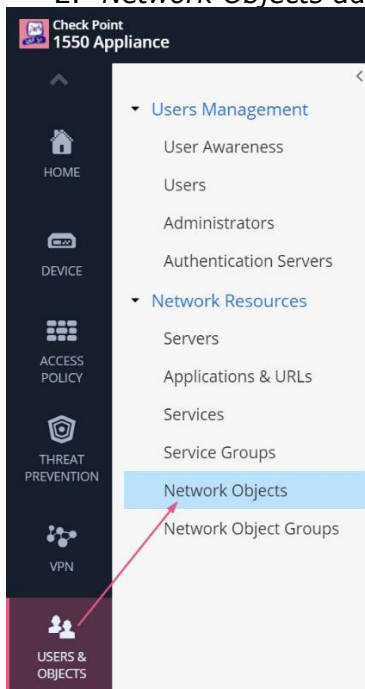
### Advanced Optionen konfigurieren:

1. *TAB Advanced* anwählen
2. Bei den Settings die Option *Remote Gateway is a Check Point Security Gateway* deaktivieren
3. Unter *Encryption method* den Parameter auf *IKEv2* stellen




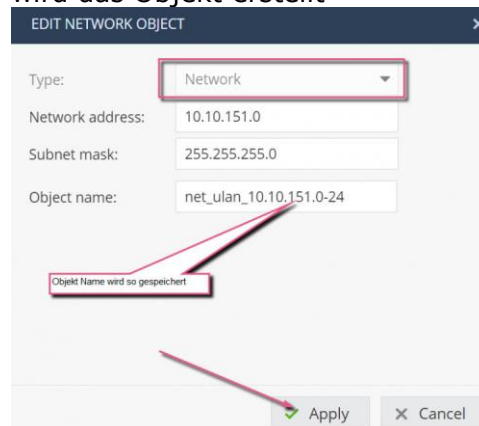
### Konfigurieren eines Netzwerk Objektes:

1. *User & Objects* anwählen
2. *Network Objects* auswählen




Im Fenster *Editor* folgendes konfigurieren:

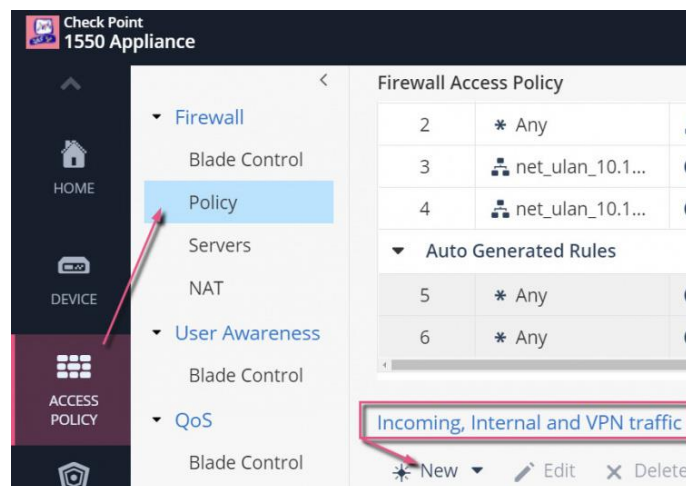
1. *Type* auf *Network* einstellen
2. *Network address*: Die Netzwerkadresse ohne Netzmaske eintragen
3. *Subnet mask*: Die Subnetzmaske des Netzes eintragen
4. *Object name*: Name des Adress-Objektes eintragen
5. Mit dem  Button wird das Objekt erstellt




### Konfigurieren der Policy:

Nun gilt es noch die Firewall Regeln zu konfigurieren:

1. Menü *Access Policy* anwählen
2. *Policy* auswählen
3. Unter dem Menü *Incoming, Internal and VPN traffic* mit  wird eine neue VPN Regel erstellt.





1. *Source* und *Destination*, wie auch die *Services* über das jeweilige Dropdown Menü im entsprechenden Feld auswählen
2. Das Feld *Match only for encrypted traffic* auswählen, so wird gewährleistet, dass diese Regel für den verschlüsselten Traffic gilt
3. Mit  **Apply** wird die Regel erstellt und aktiv:

**EDIT RULE: INCOMING, INTERNAL AND VPN TRAFFIC**



Traffic from `net_remote_10.10.161.0-24` to `net_ulan_10.10.151.0-24` on any service is accepted and logged

Source	Destination	Service	Action	Log
<code>net_remote_10.10.161.0-24</code>	<code>net_ulan_10.10.151.0-24</code>	* Any	Accept	Log

IN-VPN 10.10.161.0-24 nach Userlan 10.10.151.0-24 --- VPN Site To Site fwalem-lab-0061

☐ Apply only during this time: 09 : 00 AM - 09 : 00 AM

☒ Match only for encrypted traffic

 **Apply**  **Cancel**

4. Das Gleiche noch für die Gegenrichtung konfigurieren, falls dies vom Setup so erforderlich ist

**ADD RULE: INCOMING, INTERNAL AND VPN TRAFFIC**


Traffic from `net_ulan_10.10.151.0-24` to `net_remote_10.10.161.0-24` on any service is accepted and logged

Source	Destination	Service	Action	Log
<code>net_ulan_10.10.151.0-24</code>	<code>net_remote_10.10.161.0-24</code>	* Any	Accept	Log

OUT-VPN 10.10.151.0-24 nach Remote VPN 10.10.161.0-24 --- VPN Site To Site fwalem-lab-0061

☐ Apply only during this time: 09 : 00 AM - 09 : 00 AM

☒ Match only for encrypted traffic

 **Apply**  **Cancel**

### Regelset Anordnung:

**Incoming, Internal and VPN traffic**

**Stealth Policy (Alles auf die Checkpoint wird geblockt):**

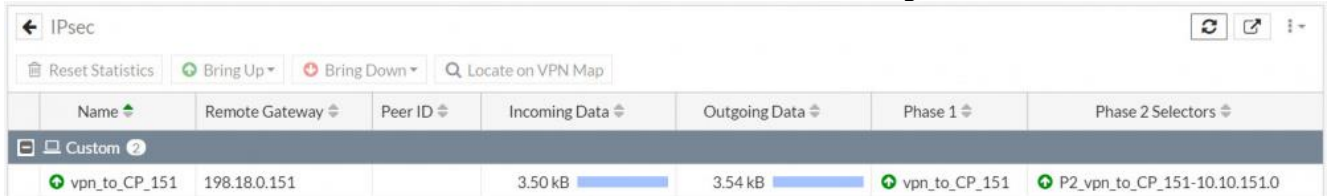
**VPN Regeln für den Tunnel zur und nach dem Netz hinter der FortiGate**

No.	Source	Destination	Service	Action	Log	Comment
1	<code>gr_also_lab_net</code>	This Gateway	* Any	Accept	Log	management A...
2	<code>fac.also-solutions...</code>	This Gateway	* Any	Accept	Log	Access For...
3	* Any	This Gateway	* Any	Block	Alert	Stealth Policy
4	<code>net_remote_10.10...</code>	<code>net_ulan_10.10.15...</code>	* Any	Accept	Log	IN-VPN 10.10.161.0-24 nach Userlan 10.10.151.0-24 --- VPN Site To Site ...
5	<code>net_ulan_10.10.15...</code>	<code>net_remote_10.10...</code>	* Any	Accept	Log	OUT-VPN 10.10.151.0-24 nach Remote VPN 10.10.161.0-24 --- VPN Site ...

## Erfolgskontrolle :

### VPN Monitor auf der FortiGate :

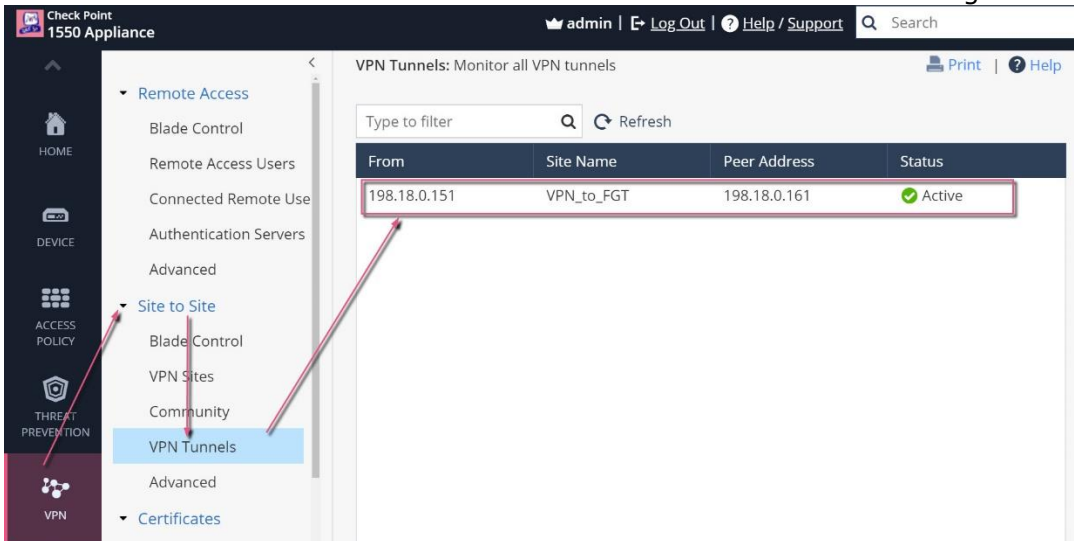
Im Menu *Dashboard* → *Network* → *IPsec* kann der VPN Monitor aufgerufen werden:



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
vpn_to_CP_151	198.18.0.151		3.50 kB	3.54 kB	vpn_to_CP_151	P2_vpn_to_CP_151-10.10.151.0

### VPN Monitor auf dem Checkpoint Gerät:

Im Menü *VPN* → *Site-to-Site* → *VPN-Tunnels* kann der VPN Monitor angeschaut werden:



From	Site Name	Peer Address	Status
198.18.0.151	VPN_to_FGT	198.18.0.161	Active

### Traffic von vom Fortinet Netz zum Checkpoint Netz:

Ping von der FortiGate aus generiert:

1. Mit dem Befehl `execute ping-option source 10.10.161.2` können wir der FortiGate angeben, mit welcher Adresse dieser Ping ausgeführt werden soll
2. Mit dem Befehl `execute ping 10.10.151.2` können wir die IP-Adresse auf der Checkpoint vom LAN Interface anpingen

```
CLI Console (1)
fwalem_lab-0061 # execute ping-option source 10.10.161.2
fwalem_lab-0061 # execute ping 10.10.151.2
PING 10.10.151.2 (10.10.151.2): 56 data bytes
64 bytes from 10.10.151.2: icmp_seq=0 ttl=64 time=1.8 ms
64 bytes from 10.10.151.2: icmp_seq=1 ttl=64 time=0.5 ms
64 bytes from 10.10.151.2: icmp_seq=2 ttl=64 time=0.5 ms
64 bytes from 10.10.151.2: icmp_seq=3 ttl=64 time=0.6 ms
64 bytes from 10.10.151.2: icmp_seq=4 ttl=64 time=0.6 ms

--- 10.10.151.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.8/1.8 ms
fwalem_lab-0061 #
```

**FortiGate diag debug flow Funktion:**

```
# diag debug flow filter clear
# diag debug flow filter sadd 10.10.161.2
# diag debug flow filter dadd 10.10.151.2
# diag debug flow trace start 900
# diag debug enable

# id=20085 trace_id=11 func=print_pkt_detail line=5639 msg="vd-root:0 received a
packet(proto=1, 10.10.161.2:3840->10.10.151.2:2048) from local. type=8, code=0,
id=3840, seq=0."
id=20085 trace_id=11 func=init_ip_session_common line=5810 msg="allocate a new
session-00098eef"
id=20085 trace_id=11 func=ipd_post_route_handler line=439 msg="out vpn_to_CP_151
vwl_zone_id 0, state2 0x0, quality 0.
"
id=20085 trace_id=11 func=ipsecdev_hard_start_xmit line=789 msg="enter IPsec
interface-vpn_to_CP_151"
id=20085 trace_id=11 func=_ipsecdev_hard_start_xmit line=666 msg="IPsec tunnel-
vpn to CP_151"
id=20085 trace_id=11 func=ipsec_common_output4 line=874 msg="SA is not ready yet,
drop"
id=20085 trace_id=12 func=print_pkt_detail line=5639 msg="vd-root:0 received a
packet(proto=1, 10.10.161.2:3840->10.10.151.2:2048) from local. type=8, code=0,
id=3840, seq=1."
id=20085 trace_id=12 func=resolve_ip_tuple_fast line=5720 msg="Find an existing
session, id-00098eef, original direction"
id=20085 trace_id=12 func=ipd_post_route_handler line=439 msg="out vpn_to_CP_151
vwl_zone_id 0, state2 0x0, quality 0.
"
..... Debug output folgendermassen unterbrechen
# diag debug reset
# diag debug disable
```

**Checkpoint fw monitor Funktion:**

```
fwalem-lab-0151> expert ← in den Expert Modus wechseln
Enter expert password:

You are in expert mode now.
FW Monitor:
[Expert@fwalem-lab-0151]# fw monitor -e 'accept host(10.10.161.2);'
fw: getting filter (from command line)
fw: compiling
monitorfilter:
Compiled OK.
fw: loading
fw: monitoring (control-C to stop)
[vs_0][fw_2] WAN:id[84]: 10.10.161.2 -> 10.10.151.2 (ICMP) len=84 id=53344
ICMP: type=8 code=0 echo request id=3840 seq=1
[vs_0][fw_2] WAN:ID[84]: 10.10.161.2 -> 10.10.151.2 (ICMP) len=84 id=53344
ICMP: type=8 code=0 echo request id=3840 seq=1
[vs_0][fw_2] WAN:o[84]: 10.10.151.2 -> 10.10.161.2 (ICMP) len=84 id=7498
ICMP: type=0 code=0 echo reply id=3840 seq=1
[vs_0][fw_2] WAN:O[84]: 10.10.151.2 -> 10.10.161.2 (ICMP) len=84 id=7498
ICMP: type=0 code=0 echo reply id=3840 seq=1
[vs_0][fw_2] WAN:O[84]: 10.10.151.2 -> 10.10.161.2 (ICMP) len=84 id=7498
ICMP: type=0 code=0 echo reply id=3840 seq=1
[vs_0][fw_2] WAN:id[84]: 10.10.161.2 -> 10.10.151.2 (ICMP) len=84 id=53345
ICMP: type=8 code=0 echo request id=3840 seq=2
[vs_0][fw_2] WAN:ID[84]: 10.10.161.2 -> 10.10.151.2 (ICMP) len=84 id=53345
ICMP: type=8 code=0 echo request id=3840 seq=2
[vs_0][fw_2] WAN:o[84]: 10.10.151.2 -> 10.10.161.2 (ICMP) len=84 id=7720
ICMP: type=0 code=0 echo reply id=3840 seq=2
[vs_0][fw_2] WAN:O[84]: 10.10.151.2 -> 10.10.161.2 (ICMP) len=84 id=7720
ICMP: type=0 code=0 echo reply id=3840 seq=2
[vs_0][fw_2] WAN:O[84]: 10.10.151.2 -> 10.10.161.2 (ICMP) len=84 id=7720
.....
Mit ctrl+c kann der output abgebrochen werden
```